

**Attachment B**

**Items to be seized related to an Animal Fighting Venture**

Evidence, fruits, and instrumentalities of violations of 7 U.S.C. § 2156(b) namely:

1. All live or dead dogs, including puppies born or unborn;
2. Other animals capable of being used in the dog fighting conditioning process;
3. All dog fighting paraphernalia, including: treadmills, cat-mills, slat mills, jenny mills, exercise wheels, hides or other material used as hanging devices to strengthen or condition dogs; collars, leashes, chains, and other devices capable of being used to exercise or restrain fighting dogs; wooden sticks or handles capable of being used to pry open dogs' jaws; breeding stands; weight scales; and any washtubs, buckets, pails, and sponges capable of being used to wash dogs;
4. Any books, magazines, photographs, film, videotapes, or writings that contain material relating to dog fighting, dog fighting conditioning, or pit bull-type dogs; including on electronically stored media;
5. Any awards, trophies, plaques, or ribbons promoting or relating to dog fighting;
6. Any film, video or audio recordings, memory cards, or other storage devices capable of recording dog fighting activity; including on electronically stored media;
7. Animal carrying cases, pens, chains, or leads;
8. Drugs or supplements capable of being used to treat injured dogs or to enhance their performance; needles and syringes capable of being used for the administration of such drugs; suture or surgical staple kits and other veterinary supplies;
9. Registration papers or other materials (written or otherwise) showing possession, ownership or transfer of dogs, including bills of sale, pedigrees, breeding records, transport

documents, shipping records, certificates, receipts, notes, and veterinary records; including on electronically stored media;

10. Any documents and records of financial accounts or transactions related to payment for or proceeds from or related to dogs, including account statements, deposits, withdrawals, checks, debits, wire transfers, or other documents; including on electronically stored media, or any cash or currency;

11. Any dog fighting records or notes, including names and telephone numbers of persons suspected of being dog fighters; any rules, contracts, conditioning logs, breeding records or other written agreements concerning the fighting of dogs; including on electronically stored media;

12. Any constructed enclosures or components of any pits or enclosures capable of being used for the purpose of dog fighting, conditioning dogs for fighting, or housing dogs intended to be used for fighting, including any carpeting or other materials used on the floor or walls of such enclosures;

13. Any dog or other animal carcasses located or buried on the property, or parts or skins thereof;

14. Any flooring or wall components displaying evidence of blood, fur, or other animal matter;

15. Any utensils or weapons capable of being utilized in the killing of animals, to include ropes, wire, guns, rifles, spent shotgun shells, spent bullet cartridges; buckets, barrels, or other devices capable of being used to drown dogs; baseball bats, metal pipes, batteries, electrical wires and clips, knives; and barrels, flammable substances, and other items capable of being used to burn live or dead dogs;

16. Devices capable of being used to deter barking in dogs, including collars, sprays, and sonic emitters;
17. Deposits of blood, fur, or other animal matter located on the property;
18. Material (e.g., from buccal (cheek) swabs) for DNA determination from all live dogs for purposes of comparison with other blood/tissue evidence;
19. Any and all materials reflecting the destruction of evidence at that location, including destroyed, damaged, or tampered with documents, flooring, wall components, or other structures;
20. Soil, blood, fur, animal skins and vegetation from the property to be used for forensic testing; and
21. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;

- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. Contextual information necessary to understand the evidence described in this attachment.

22. In order to search for the items described above that may be maintained in electronic media, law enforcement personnel are authorized to search, copy, image and seize the following items for off-site review:

- a. any computer or storage medium capable of being used to commit, further or store evidence of the federal offenses listed above; and

b. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

23. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

24. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

25. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

26. For purposes of authentication at trial, the Government is authorized to retain a digital copy of all seized information authorized by the Warrant for as long as is necessary for authentication purposes.

27. Any computers and peripherals or storage devices, which are seized pursuant to this warrant, will be reviewed, analyzed, imaged, or copied so that, if no contraband is found on the seized computer devices, the computer or other devices can be returned to the owner of the devices. Any images or copies made may be retained and analyzed consistent with the provisions of the search warrant, but no device determined to contain contraband need be returned and may be retained. If the imaging or analysis is not completed so that a determination can be made

whether the devices can be returned within 45 days of execution of the warrant, the agent executing the warrant will report the status of such imaging or analysis to the Court. The agent will thereafter report to the Court on the status every 30 days until the devices are returned or a determination is made that the devices contain contraband.